

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, James V. Richardson, being duly sworn, depose and state as follows:

INTRODUCTION

1. I am a Special Agent with United States Department of Homeland Security (DHS), Immigrations and Customs Enforcement (ICE), Homeland Security Investigations (HSI), and am assigned to the office of the Resident Agent in Charge, Providence, RI. I have been an agent of HSI since 2009. As part of my duties, I am authorized to investigate violations of the laws of the United States, including criminal violations relating to child exploitation, child pornography, coercion and enticement, and transportation of minors, and the transfer of obscene material to minors, including but not limited to, violations of 18 U.S.C. §§ 2252, and 2252A. I have received training in the investigation of child pornography, child exploitation, and transportation of minors, and have had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256).

2. I am currently participating in an investigation relating to violations of federal law by Anthony NINFO (DOB XX/XX/1981) for possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct in violation of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) and distribution of child pornography in violation of 18 U.S.C. §§ 2252(a)(2) and (b)(1). I submit this affidavit in support of an application to search the person of Anthony NINFO (hereinafter “NINFO”) and NINFO’s residence, the premises located at 787 Providence Street, West Warwick, RI 02893 (the “SUBJECT PREMISES”), and the content of any electronic media storage devices or media located therein, as more fully described in Attachment A, which is incorporated herein by reference; and to seize evidence,

instrumentalities, fruits of crime, and contraband as more fully described in Attachment B, which is also incorporated herein by reference.

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

3. In October 2020, Homeland Security Investigations (HSI) Canberra received an investigative referral from New Zealand Customs Service (NZCS). The referral originated from a NZCS investigation into users of Mega.nz, a file sharing website.

4. In September 2020, the NZCS executed a search warrant and retained a Mega.nz account. During analysis of that account, a user named “*anne smith*” was identified as having distributed child pornography. Internet Protocol (IP) logs were obtained which indicate user “*anne smith*” to be in the District of Rhode Island.

5. Analysis of the “*anne smith*” Mega.nz account identified that between the 28th of October 2019 to the 6th of January 2020, user “*anne smith*” distributed 3 images of child pornography and received 4 images of child pornography via a private chat with another user. I reviewed the images provided to me by HSI Canberra and confirmed that they are consistent with the federal definition of child pornography. The following are descriptions of images sent/received by user “*anne smith*”:

- a. File name: 2019-04-22 23.01.17.jpg

Description: The jpg image file depicts two nude prepubescent females with their legs spread exposing their vaginas and anus.

- b. File name: 2019-04-22 23.17.54.jpg

Description: The jpg image file depicts the graphic and lascivious display of a prepubescent female’s vagina. An adults hands are spreading the vagina apart.

- c. File name: Avatar_user953213_851950395282257.jpg

Description: The jpg image file depicts a penis penetrating the anus of a nude prepubescent female.

6. As part of the information obtained from Mega.nz by the NZCS was the email address xsucidexkingx@hotmail.com which is associated with user “*anne smith*”. On October 27, 2020, HSI Canberra submitted a Department of Homeland Security (DHS) Summons (0J-21-026) to Microsoft Corporation requesting subscriber information on xsucidexkingx@hotmail.com.

7. On October 29, 2020, Microsoft provided the following response:

Registration Profile:

Signin name: xsucidexkingx@hotmail.com

First Name: Anthony

Last Name: N

Region: North Carolina

Postal Code: 28394

Creation Date: 11/15/2003

Alias: piercedinked@yahoo.com

IP History:

Address: 72.192.13.42

Date: 10/8/2020 at 16:10 UTC

8. On November 1, 2020, using the IP information provided in the Microsoft response, HSI Canberra submitted DHS Summons 0J-21-0343 to Cox Communications requesting subscriber information on IP address 73.192.13.42.

9. On November 16, 2020, Cox Communications provided the following response:

Subscriber Info:

Name: Corallea Palazzo

Address: Unit 21, 787 Providence St, West Warwick, RI 02893

Phone(s): 401-699-2428, 401-615-5841, and 401-378-5952

MAC: C0:C5:22:FE:AC:BA

10. A search of a public records database that provides names, dates of birth, addresses, associates, telephone numbers, email addresses, and other information was conducted for the SUBJECT PREMISES. These public records indicated that Anthony NINFO and Corallea Palazzo currently reside at the address. The same database also indicate that NINFO previously resided in North Carolina.

11. A check with the Department of Motor Vehicles on or about April 22, 2021 revealed that Anthony NINFO and Corallea Palazzo all reside at the SUBJECT PREMISES.

12. The U.S. Postal Service confirmed that Anthony NINFO and Corallea Palazzo are both currently receiving mail at the SUBJECT PREMISES.

13. Social media queries (Facebook) revealed the username *corallea.palazzo* is 'in a relationship' with user *anthony.ninfo*. Both usernames show as residing in West Warwick, RI. In addition, the *corallea.palazzo* profile pictures shows a woman with a child.

14. On April 20, 2021, I conducted surveillance of the SUBJECT PREMISES. The SUBJECT PREMISES appear to be a multi-level apartment building, white in color. There are 4 mailboxes on the front of the house. The top mailbox to the left of the front door has the number “787” clearly affixed to the house directly above the mailbox.

**CHARACTERISTICS COMMON TO PERSONS WHO ENGAGE IN
CHILD SEXUAL EXPLOITATION**

15. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have collaborated, I have learned that there are certain characteristics that are generally common to offenders who access, send, distribute, exhibit, possess, display, transport, manufacture, or produce material which depicts minors engaged in sexually explicit conduct, or who engage in sexually explicit communications with minors. Said material includes, but is not limited to, photographs and videos stored electronically on computers, digital devices, or related digital storage media.

16. Such offenders may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have that stem from viewing children engaged in sexual activity or in sexually suggestive poses, whether in person, in photographs or other visual media, or from literature describing such activity.

17. Such offenders may collect sexually explicit or suggestive materials in a variety of media, including digital photographs, videos, or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to facilitate contact offenses – that is, to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

18. Such offenders almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain their cache for many years. In my training and experience, I am aware that such offenders often

19. Likewise, such individuals often maintain their child pornography images in a

digital or electronic format in a safe, secure, and private environment, such as a, “SD card,” computer or surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the offender’s residence, inside the offender’s vehicle, or, at times, on his person, to enable the individual to view the child pornography images, which are highly valued.¹

20. Some of these individuals, however, have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis, presumably to avoid criminal liability. Importantly, as described in more detail below, evidence of such activity, including deleted child pornography, often can be located on these individuals’ computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual “deleted” it.²

21. Such offenders also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists or other record of individuals with whom they have been in contact and who share the same interests in child pornography.

22. Such offenders prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if such an offender uses a

¹ See *United States v. Morales-Aldahondo*, 524 F.3d 115, 117-119 (1st Cir. 2008) (3-year delay between last download and warrant application not too long, given affiant testimony that consumers of child pornography value collections and thus often retain them for a period of time, and consumers who use computers to access child pornography are likely to use computers to store their collections);

² See *United States v. Seiver*, 692 F.3d 774, 775-776 (7th Cir. 2012) (in context of staleness challenge, collecting and agreeing with cases from the 4th, 5th, 6th, and 9th Circuits that acknowledge the ability of forensic examiners to recover evidence of child pornography even after such files are deleted by a user).

portable device (such as a mobile phone or gaming device) to access the internet and child pornography, it is more likely than not that evidence of this access will be found in his home – here, the SUBJECT PREMISES, as set forth in Attachment A.

23. Based upon the foregoing, I believe that David C. NINFO likely displays characteristics common to individuals who access with the intent to view and possess, collect, receive, or distribute child pornography. As such, I submit that there is probable cause to believe that contraband material depicting minors engaged in sexually explicit conduct and other evidence, instrumentalities, and fruits of violations of possession and access with intent to view child pornography 18 U.S.C. §§ 2252(a)(4) exist at the SUBJECT PREMISES, in addition to evidence of attempted enticement of a minor in violation of 18 U.S.C. §2422(b).

SEARCH AND SEIZURE OF COMPUTER SYSTEMS AND DATA

24. Based on my knowledge, training, experience, and information provided to me by other agents, I know that computer files or remnants of such files can be recovered months or even years after they have been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from an old computer to a new computer.

b. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, computer storage media – in particular, computers' internal hard drives – contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is usually required for that task.

d. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.” The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

25. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software, or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, computer-related documentation, and storage media (“computer equipment”) be seized and subsequently processed by a qualified computer specialist in a laboratory setting, rather than in the location where it is seized. This is true because of:

a. The volume of evidence: Storage media such as hard disks, SD cards, flash drives, CD-ROMs, and DVD-ROMs can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine what particular files are evidence, fruits, or instrumentalities of criminal activity.

This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.

b. Technical requirements: Analyzing computer hardware, computer software, or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even “hidden,” deleted, compressed, password-protected, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a “booby trap.”

BIOMETRIC ACCESS TO DEVICES

26. This warrant permits law enforcement to compel Anthony NINFO to unlock any DEVICES requiring biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:

- a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices

offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

- b.** If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.
- c.** If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called “Trusted Face.” During the Trusted Face registration process, the user holds the device in front of his or her face. The device’s front-facing camera then analyzes and records data based on the user’s facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.
- d.** If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called “Windows Hello.” During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or

her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

- e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.
- f. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the DEVICES subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the DEVICES, making the use of biometric features necessary to the execution of the search authorized by this warrant.
- g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or

has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours *and* the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

- h.** Due to the foregoing, if law enforcement personnel encounter any DEVICES that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of Anthony NINFO to the fingerprint scanner of the DEVICES found at the premises; (2) hold the DEVICES found at the premises in front of the face of Anthony NINFO and activate the facial recognition feature; and/or (3) hold the DEVICES found at the premises in front of the face of Anthony NINFO and activate the iris recognition feature, for the purpose of attempting to unlock the DEVICES in order to search the contents as authorized by this warrant. The proposed warrant does not authorize law enforcement to compel that Anthony NINFO state or otherwise provide the password or any other means that may be used to unlock or access the DEVICES. Moreover, the proposed warrant does not authorize law enforcement to compel Anthony NINFO to identify the specific biometric characteristics (including the

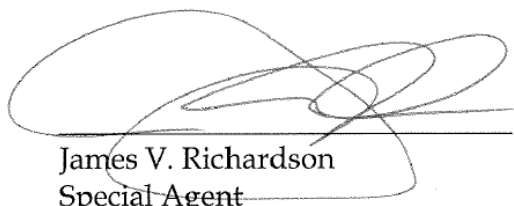
unique finger(s) or other physical features) that may be used to unlock or access the DEVICES.

CONCLUSION

27. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the locations described in Attachment A. I respectfully request that this Court issue a search warrant for the locations described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

28. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the “return” inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

Sworn to under the pains and penalties of perjury,


James V. Richardson
Special Agent
Homeland Security

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1
by:

telephone
(specify reliable electronic means)

Date

Judge's signature

Providence, Rhode Island
City and State

Patricia A. Sullivan, US Magistrate Judge
Printed name and title

ATTACHMENT A
DESCRIPTION OF LOCATION TO BE SEARCHED

The premises to be searched include:

- A. The person of Anthony NINFO, a white male, standing 6'07", born in 1981.
- B. The content of any electronic media storage devices, including smart phones, or media located on the person of Anthony NINFO or found in the premises of 787 Providence Street, West Warwick, RI 02893.
- C. Premises located at 787 Providence Street, West Warwick, RI 02893, more particularly described as a white multi-story apartment building. The number "787" is clearly marked above a mailbox to the left of the front door. The exterior of the premises is pictured below:



ATTACHMENT B
DESCRIPTION OF INFORMATION TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) and 18 U.S.C. §§ 2252(a)(2) and (b)(1):

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which are stored records or information that is otherwise called for by this warrant (hereinafter, “COMPUTER”):
 - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved user names and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the lack of such malicious software;
 - d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;
 - e. evidence indicating the computer user’s knowledge and/or intent as it relates to the

- crime(s) under investigation;
 - f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
 - g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;
 - h. evidence of the times the COMPUTER was used;
 - i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
 - j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
 - k. records of or information about Internet Protocol addresses used by the COMPUTER;
 - l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
 - m. contextual information necessary to understand the evidence described in this attachment.
3. Routers, modems, and network equipment used to connect computers to the Internet.
 4. Child pornography, as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2), and child erotica.
 5. Records, information, and items relating to violations of the statutes described above including:
 - a. Records, information, and items relating to the occupancy or ownership of the

SUBJECT PREMISES, including utility and telephone bills, mail envelopes, or addressed correspondence;

- b. Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;
- c. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;
- d. Records and information relating to sexual exploitation of children, including correspondence and communications between users of child pornography and exploitation websites.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

During the execution of the search of the PREMISES described in Attachment A, law enforcement personnel are also specifically authorized to compel Anthony NINFO to provide biometric features, including pressing fingers (including thumbs) against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, of:

- (a) any of the DEVICES found at the PREMISES, and
- (b) where the DEVICES are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,

for the purpose of attempting to unlock the DEVICES' security features in order to search the contents as authorized by this warrant.

This warrant does not authorize law enforcement personnel to compel any other individuals found at the PREMISES to provide biometric features, as described in the preceding paragraph, to access or otherwise unlock any DEVICE. Further, this warrant does not authorize law enforcement personnel to request that Anthony NINFO to state or otherwise provide the password or any other means that may be used to unlock or access the DEVICES, including by identifying the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the DEVICES.

DEFINITIONS

For the purpose of this warrant:

- A. "Computer equipment" means any computer hardware, computer software, computer-related documentation, storage media, and data.
- B. "Computer hardware" means any electronic device capable of data processing (such as a computer, gaming device, smartphone, cellular telephone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).
- C. "Computer software" means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.
- D. "Computer related documentation" means any material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.
- E. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).
- F. "Data" means all information stored on storage media of any form in any storage format and for any purpose.
- G. "A record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.

H. “Obscene material” is any image or video representation containing material which the average person, applying contemporary community standards would find that the work, taken as a whole, appeals to the prurient interest; depicts in a patently offensive way, sexual conduct and taken as a whole, lacks serious literary, artistic, political, or scientific value such as patently offensive representations or descriptions of ultimate sexual acts, normal or perverted, actual or simulated, patently offensive representation or descriptions of masturbation, excretory functions, and lewd exhibition of the genitals.